DAU-AM-12-207

ACQUISITION RESEARCH SPONSORED REPORT SERIES

A Survey and Study of the Risk Behavior of the DoD Workforce

25 October 2012

by

Dr. Donald McKeon, Professor

Defense Acquisition University (DAU)

Prepared for: Naval Postgraduate School, Monterey, California 93943

ACQUISITION RESEARCH PROGRAM
GRADUATE SCHOOL OF BUSINESS & PUBLIC POLICY
NAVAL POSTGRADUATE SCHOOL

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
25 OCT 2012		**00-00-2012 to 00-00-2012**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
A Survey and Study of the Risk Behavior of the DoD Workforce	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Defense Acquisition University (DAU),9820 Belvoir Road,Fort Belvoir,VA,22060-5565**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

This research project examines the behavior of the Department of Defense (DoD) workforce hypothesis regarding risk management in weapon system development. A survey was conducted to understand how the workforce approaches risk management. Many DoD programs fall behind and suffer a cost increase and schedule delay. A recent Government Accountability Office (GAO; 2012) report stated, ?The total cost of DOD?s 2011 portfolio of major defense acquisition programs has grown by ? 5 percent, in the last year.?(p. 6) In addition, when compared to a program?s initial plans, the cost increase is much larger: ?When measured from their first full estimates, ? the growth in total acquisition cost for these programs is ? 40 percent.? (p. 6) Risk management is an important engineering tool for minimizing the impact of technical problems of a program. More effective risk management will lead to better managed programs. The purpose of this study is to better understand the DOD?s workforce?s attitude towards risk management and risk mitigation. Findings of the study will aid in improving training on risk management in order to improve the overall performance of weapon system programs. This research project is based on an online survey sent to 420 members of the DoD acquisition workforce. The survey was completed by 87 DoD workforce members in an acquisition position. The experience level of the survey participants was high, with 66% of the participants having six or more years of experience, and an average experience level for all participants of 11.0 yrs. Only 55% of the participants knew of a risk management plan for their organization. Three scenarios requiring a decision about the level of mitigation were presented to the participants. While there wasn?t a single right answer to the three scenarios, the participants? decisions should have been based on factors such as the product price, failure rate, likelihood of obsolescence, new technology, criticality to the mission, and so forth. However, a finding from the research is that there was a wide variation in responses to the scenarios, from not spending any on mitigation to spending an amount equal to the total value of the product or service. That is, there was no consistency in deciding on the risk mitigation plan. The participants identified important activities required for successful risk management. The seven activities named most frequently by participants were directly or indirectly related to the effectiveness of doing risk management. The activities were  analysis and assessment (97%)  cooperation from others (97%)  subject matter expert (SME) advice (95%)  mitigation planning (93%)  detailed risk management plan (92%)  training (82%), and  expertise in risk management (79%). Future

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**71**	

The research presented in this report was supported by the Acquisition Chair of the Graduate School of Business & Public Policy at the Naval Postgraduate School.

To request Defense Acquisition Research or to become a research sponsor, please contact:

NPS Acquisition Research Program
Attn: James B. Greene, RADM, USN, (Ret.)
Acquisition Chair
Graduate School of Business and Public Policy
Naval Postgraduate School
555 Dyer Road, Room 332
Monterey, CA 93943-5103
Tel: (831) 656-2092
Fax: (831) 656-2253
E-mail: jbgreene@nps.edu

Copies of the Acquisition Sponsored Research Reports may be printed from our website: www.acquisitionresearch.net

ACQUISITION RESEARCH PROGRAM
GRADUATE SCHOOL OF BUSINESS & PUBLIC POLICY
NAVAL POSTGRADUATE SCHOOL

Abstract

This research project examines the behavior of the Department of Defense (DoD) workforce hypothesis regarding risk management in weapon system development. A survey was conducted to understand how the workforce approaches risk management.

Many DoD programs fall behind and suffer a cost increase and schedule delay. A recent Government Accountability Office (GAO; 2012) report stated, “The total cost of DOD’s 2011 portfolio of major defense acquisition programs has grown by … 5 percent, in the last year.”(p. 6) In addition, when compared to a program’s initial plans, the cost increase is much larger: “When measured from their first full estimates, … the growth in total acquisition cost for these programs is … 40 percent.” (p. 6)

Risk management is an important engineering tool for minimizing the impact of technical problems of a program. More effective risk management will lead to better managed programs. The purpose of this study is to better understand the DOD’s workforce’s attitude towards risk management and risk mitigation. Findings of the study will aid in improving training on risk management in order to improve the overall performance of weapon system programs.

This research project is based on an online survey sent to 420 members of the DoD acquisition workforce. The survey was completed by 87 DoD workforce members in an acquisition position. The experience level of the survey participants was high, with 66% of the participants having six or more years of experience, and an average experience level for all participants of 11.0 yrs.

Only 55% of the participants knew of a risk management plan for their organization. Three scenarios requiring a decision about the level of mitigation were presented to the participants. While there wasn’t a single right answer to the three

scenarios, the participants' decisions should have been based on factors such as the product price, failure rate, likelihood of obsolescence, new technology, criticality to the mission, and so forth.

However, a finding from the research is that there was a wide variation in responses to the scenarios, from not spending any on mitigation to spending an amount equal to the total value of the product or service. That is, there was no consistency in deciding on the risk mitigation plan.

The participants identified important activities required for successful risk management. The seven activities named most frequently by participants were directly or indirectly related to the effectiveness of doing risk management. The activities were

- analysis and assessment (97%),
- cooperation from others (97%),
- subject matter expert (SME) advice (95%),
- mitigation planning (93%),
- detailed risk management plan (92%),
- training (82%), and
- expertise in risk management (79%).

Future training activities should include performing the above activities. While risk management is taught in many Defense Acquisition University (DAU) classes, the training needs to go beyond understanding likelihood, consequence, and future root cause and needs to develop skills in the seven areas described previously.

Keywords: DoD workforce, risk management, online survey

About the Author

Dr. Donald McKeon is a Defense Acquisition University (DAU) professor of systems engineering management and is located in Warren, MI, supporting the Tank-Automotive and Armaments Command–Life Cycle Management Command (TACOM–LCMC). Dr. McKeon teaches systems engineering, manufacturing and quality, software acquisition management, program management, and performance-based contracting. He has consulted on programs for the Air Force and the Army. Prior to joining DAU, Dr. McKeon worked in research at Sandia National Laboratories and in product development and manufacturing in private industry. Dr. McKeon has a BS, MS, and PhD in engineering and an MBA.

Donald McKeon, PhD, Professor
Defense Acquisition University
Tel: (586) 276-2172
Fax: (586) 264-0069
E-mail: don.mckeon@dau.mil

THIS PAGE INTENTIONALLY LEFT BLANK

DAU-AM-12-207

ACQUISITION RESEARCH SPONSORED REPORT SERIES

A Survey and Study of the Risk Behavior of the DoD Workforce

25 October 2012

by

Dr. Donald McKeon, Professor

Defense Acquisition University (DAU)

THIS PAGE INTENTIONALLY LEFT BLANK

Table of Contents

THIS PAGE INTENTIONALLY LEFT BLANK

List of Figures

THIS PAGE INTENTIONALLY LEFT BLANK

Glossary of Acronyms and Terms

ACQ 450 ..... "Leading in the Acquisition Environment" course taught by DAU
ACQ 451 ..... "Integrated Acquisition for Decision Makers" course taught by DAU
ACQ 452 ..... "Forging Stakeholder Relationships" course taught by DAU
ACQ-101 ..... "Fundamentals of Systems Acquisition Management" taught by DAU
ACQ-201 ..... "Intermediate Systems Acquisition" taught by DAU (includes ACQ-201A and ACQ-201B)
ACQ-201A ..... "Intermediate Systems Acquisition, Part A" taught by DAU
ARM ..... Active Risk Manager
AT&L ..... Acquisition, Technology, and Logistics
BLRIP ..... Beyond Low Rate Initial Production Report
CAT-I ..... Category
DAG ..... Defense Acquisition Guidebook
DAU ..... Defense Acquisition University
DAWIA ..... Defense Acquisition Workforce Improvement Act
DCMA ..... Defense Contract Management Agency
DoD ..... Department of Defense
DoDD ..... Department of Defense Directive
DOORS ..... DOORS is a requirement management software tool
FMEA ..... Failure Mode and Effect Analysis
FY2006 ..... Fiscal Year 2006
GAO ..... Government Accountability Office
GCS ..... Ground Combat Systems
GPQ ..... Group Process Questionnaire
H0 ..... Null Hypothesis
H1 ..... Alternate Hypothesis
IA ..... Information Assurance
IEEE ..... Institute of Electrical and Electronics Engineers
IPPD ..... Integrated Product and Process Development
IPT ..... Integrated Product Team
IT ..... Information Technology
LCMC ..... Life-Cycle Management Command
LOG ..... Logistics
LTU ..... Lawrence Technological University
MDA ..... Milestone Decision Authority

MIPR ..... Military Interdepartmental Purchase Request
OSD ..... Office of the Secretary of Defense
OUSD(AT&L) .... Office of the Under Secretary of Defense (Acquisition, Technology, and Logistics)
PEO ..... Program Executive Office
PM ..... Program Manager
PMT 401 ..... Program Manager's Course taught by DAU
R&D ..... Research & Development
RFI ..... Request for Information
RFP ..... Request for Proposal
RM ..... Risk Management
SME ..... Subject Matter Expert
SPRDE ..... Systems Planning, Research Development, and Engineering
SSCF ..... Senior Service College Fellowship Program
SYS-203 ..... "Intermediate Systems Planning, Research, Development, and Engineering, Part II" course taught by DAU
SYS-302 ..... "Technical Leadership in Systems Engineering" course taught by DAU
TACOM ..... Formerly known as Tank-Automotive and Armaments Command, now called the TACOM LCMC. It includes several organizations.
URL ..... Uniform Resource Locator
USD(AT&L) ..... Under Secretary of Defense for Acquisition, Technology, and Logistics

I. Introduction

This research project examines the behavior of the Department of Defense (DoD) workforce hypothesis regarding risk management in weapon system development. A survey was conducted to understand how the workforce approaches risk management. The results will lead to more effective training of the workforce.

A. Background

Many DoD programs fall behind and suffer a cost increase and schedule delay. A recent Government Accountability Office (GAO; 2012) report stated,

> The total cost of DOD's 2011 portfolio of major defense acquisition programs has grown by over $74 billion, or 5 percent, in the last year. The over $74.4 billion in cost growth over the past year consists of a rise in development costs of $13.7 billion, or 4 percent, and an increase in procurement costs of $60.6 billion, or 5 percent. (p. 6)

In addition, when compared to a program's initial plans, the cost increase is much larger:

> When measured from their first full estimates, which have been put in place over a number of years, the growth in total acquisition cost for these programs is $447 billion, or 40 percent. (GAO, 2012, p. 2)

Furthermore, from the same GAO (2012, p. 2) report,

> We found that most of these future programs are implementing acquisition reforms, such as competitive prototyping, early systems engineering reviews, and acquisition strategies ensuring competition or the option of competition, which have the potential to reduce risk and improve outcomes. Some of these activities require higher upfront investments in systems engineering and other areas to reduce longer term development risk, and it will be important for decision makers to sustain these investments when appropriate, even as DOD's budgetary resources shrink.

Finally, the following was written in the 2012 GAO report:

> … overall, most of the 37 programs we assessed are not fully adhering to a knowledge-based approach, putting them at higher risk of cost growth and schedule delays. (p. 22)

B. Problem Statement

DoD major weapon system programs continue to experience cost overruns and schedule delays. Risk management is an important engineering tool for minimizing the impact of technical problems of a program. More effective risk management will lead to better managed programs.

C. Purpose of this Study

The purpose of this study is to better understand the DOD's workforce's attitude towards risk management and risk mitigation. Findings of the study will aid in improving training on risk management in order to improve the overall performance of weapon system programs.

D. Research Hypothesis

The hypothesis of this research paper is as follows:

- The DoD workforce does not make data-driven decisions in risk management.

E. Research Methodology

This research project is based on an online survey sent to 420 members of the DoD acquisition workforce.

F. Objectives and Outcomes

The desired outcome is to make recommendations on improvements to the risk management process and improvements to training on risk management and mitigation.

G. Limitations of the Study

The research project is based on a sample of Defense Acquisition University (DAU) students in the Defense Acquisition Workforce Improvement Act (DAWIA) career fields. The majority of the sample group are in the Systems Planning, Research Development, and Engineering (SPRDE) or Logistics (LOG) career fields. Furthermore, 75% of the survey participants are military or civilian members of the Army. The survey was completed by 88 DAU students, which is a small percentage of the total DAWIA population (150,566 at the end of March 2011).

H. Reliability of the Responses

The reliability of the responses is high. The survey participants voluntarily participated in the survey and the survey was anonymous.

THIS PAGE INTENTIONALLY LEFT BLANK

II. Literature Review

A. Risk

Blanchard and Fabrycky (2011, p. 690) explained risk in this way: "Risk is the potential that something will go wrong as a result of one or a series of events."

The DoD (2006, p. 1) defined risk in the *DoD Risk Management Guide* as follows:

> Risk is a measure of future uncertainties in achieving program performance goals and objectives within defined cost, schedule and performance constraints. Risk can be associated with all aspects of a program (e.g., threat, technology maturity, supplier capability, design maturation, performance against plan [sic]) as these aspects relate across the Work Breakdown Structure (WBS) and Integrated Master Schedule (IMS). Risk addresses the potential variation in the planned approach and its expected outcome. While such variation could include positive as well as negative effects, this guide will only address negative future effects since programs have typically experienced difficulty in this area during the acquisition process.
>
> Risks have the following three components:
>
> - a future root cause (yet to happen), which, if eliminated or corrected, would prevent a potential consequence from occurring;
> - a probability (or likelihood) assessed at the present time of that future root cause occurring; and
> - the consequence (or effect) of that future occurrence.
>
> A future root cause is the most basic reason for the presence of a risk. Accordingly, risks should be tied to future root causes and their effects.

Charette (1989, p. 52) explained risk as follows:

> The definition of the word "risk" also makes a very clear statement that there will be a chance of loss associated with it. For instance, a sure loss is not a risk, because it has a certainty of occurrence. In "certainty situations," the gains and benefits can be objectively traded straightforwardly against the

losses or costs that exist. Thus, decisions are not influenced by a lack of information about the situation.

Uncertainty, on the other hand, exists in the absence of information about past, present and future events, values or conditions. This means there is a lack of confidence in the correctness of the estimated probability distribution.

Charette (1989, p. 55) went on to explain, "For an event, action, thing, etc. to be considered a risk, there must be:

- A loss associated with it
- Uncertainty or chance involved
- Some choice involved."

In *An Anatomy of Risk*, Rowe (1977, p. 24) said, "Risk is the potential for realization of unwanted, negative consequences of an event."

Sir David Cox made an important point (as cited in Vose, 2008, p. 47): "Variability is a phenomenon in the physical world to be measured, analyzed and where appropriate explained. By contrast, uncertainty is an aspect of knowledge."

Vose (2008, p. 48) described uncertainty as follows: "Uncertainty is the assessor's lack of knowledge … about the parameters that characterize the physical system that is being modeled."

Barkley (2004) explained risk management in several ways:

Project risk management is an art, not a science. I have always been skeptical of scientific and overly quantitative answers to complex social, organizational and project outcomes, especially when customers, product and markets are involved. (p. xvii)

Risk is no longer looked at as a single project issue…(p. 70)

Over emphasis on quantitative tools and mathematical models suggests risk management as a science rather than an art. (p. 70)

Grey (1995, p. 69) wrote,

> Human estimators will always be drawing on past experience, their own and that of other people, and adjusting it to allow for the special factors of the case they are now looking at. No estimate is untouched by human hand. Even historical data have been cleaned up and adjusted before anyone can use them.

B. Survey on Risk Management or Risk Mitigation by the DoD Workforce

A paper or article on the risk behavior of the DoD workforce was not found during the literature-search phase of this project.

THIS PAGE INTENTIONALLY LEFT BLANK

III. Research Methodology

A. Research Hypothesis

The hypothesis of this research paper is as follows:

- The DoD workforce does not make data-driven decisions in risk management.

B. Research Survey

The desire of this research project was to provide a repeatable survey instrument that could be used to assess the DoD workforce's attitude to risk management. A survey was chosen over interviews because the survey generated more input from the DoD workforce. The survey also provided an objective measure of the workforce's attitude toward risk management.

A drawback of a survey over interviews is that any ambiguity in a question cannot be addressed while the participant is taking the survey. To minimize this potential problem, the survey was tested by faculty members at DAU–Midwest region, and their suggestions were incorporated into the survey.

The survey was sent to 420 DAU students. The students came from 12 classes held within the six months prior to the survey and two classes that were scheduled to be completed in the two months following the survey period.

The SurveyMonkey survey tool[1] was used to generate the survey. The survey URL link was sent to the students using the author's "@dau.mil" email address to demonstrate that the survey request was a legitimate request from a government employee.

[1] The SurveyMonkey survey tool (available at http://surveymonkey.com) was used for this research project.

The survey was left open for three weeks in April 2012.

C. Data Collection

While SurveyMonkey can be used for data analysis, the author downloaded all of the data into an Excel file for data analysis because of the many capabilities of Excel.

Ninety-one people accessed the survey, although not everyone completed the survey. Figure 1 shows the number of participants answering each question of the survey.[2] Eight-seven people started the survey (Question 2), and 74 participants answered all 29 questions. The response rate for taking the survey was 21%.

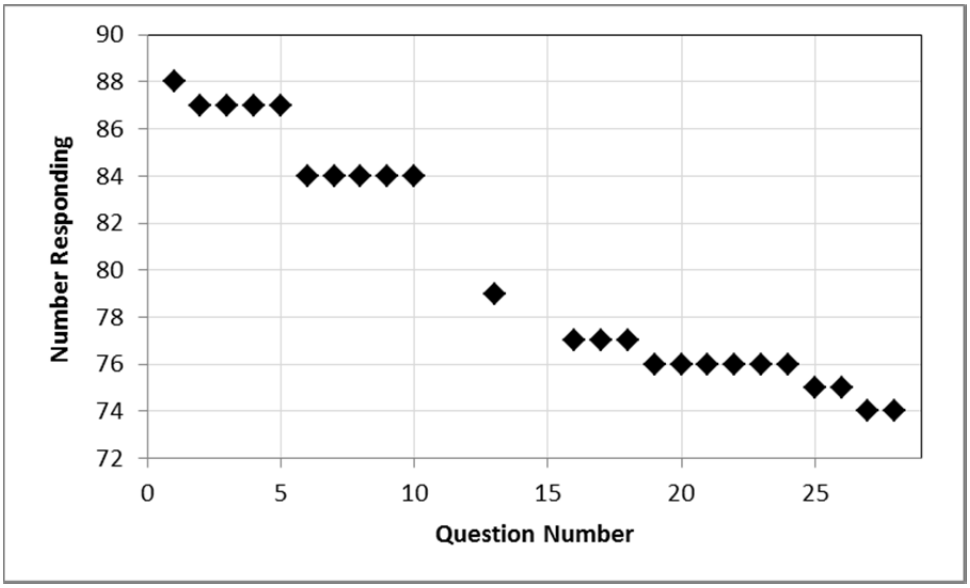

Figure 1. Number of Students Who Answered Each Survey Question

[2] Some questions allowed more than one response and were not counted.

IV. Analyzing the Data and Reporting Results

In this section, the raw data from the survey results are presented. Findings of the research are presented in Chapter 5.

The following are the purposes of the survey:

1. Identify who was taking the survey (agency, career field, experience level);
2. Identify if the employee worked in a group that used risk management (e.g., process, mitigation plan, review board, and software tool);
3. Identify the participants' job responsibilities;
4. Describe the frequency of risk mitigation steps;
5. Identify the importance of certain activities for successful risk management; and
6. Identify the risk behavior of the participants by asking them questions regarding five scenarios about risk mitigation.

The following sections present the data from the survey.

Q2—Participants by Career Field

The distribution of the participants by career field (see Figure 2) was heavily populated (64%) by workforce members in the SPRDE career field. This was expected because the survey was sent to students from eight systems engineering classes. The next largest group was the Logistics (LOG) career field with 18%. The remaining respondents were made up of the other[3] career fields.

3 AUD—Auditing; BCF—Business, Cost Estimating, and Financial Management; CON—Contracting; Facilities Engineering; IND—Industrial Property Management; IT—Information Technology; LOG—Life Cycle Logistics; PQM—Production, Quality, and Manufacturing; PM—Program Management; Purchasing; SRPDE—Systems Planning, Research, Development, and Engineering; T&E—Test and Evaluation.

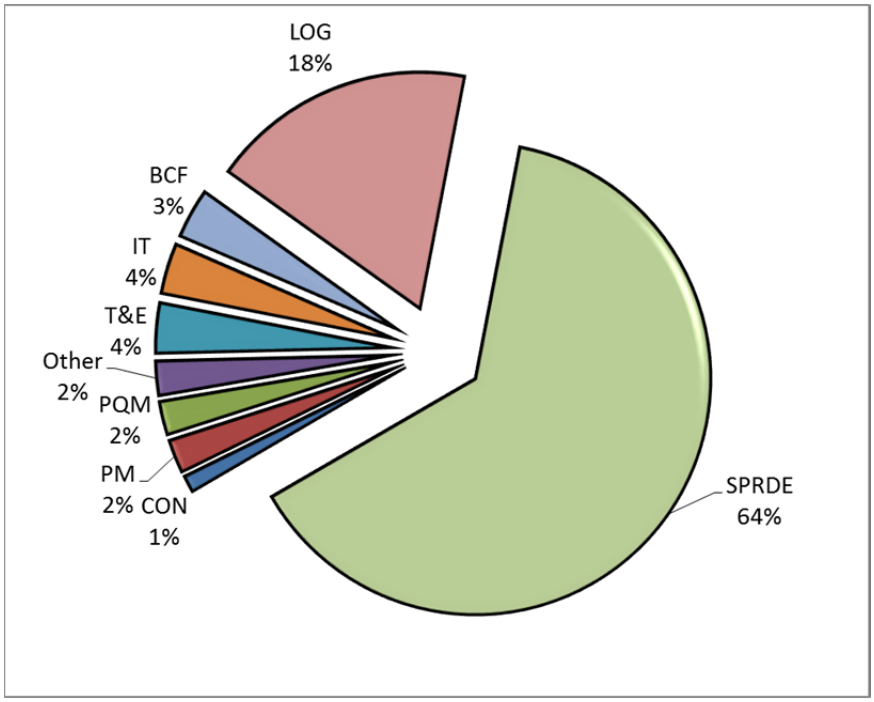

Figure 2. Breakdown of Students Participating in the Survey by Career Field

Q3—Participants by the Number of Years of Experience

Question 3 asked participants about their total number of years of professional experience, either in the civilian government workforce, the military, or any industry (see Figure 3). Sixty-six percent (66%) had more than five years of experience, while only 15% had less than two years of experience.

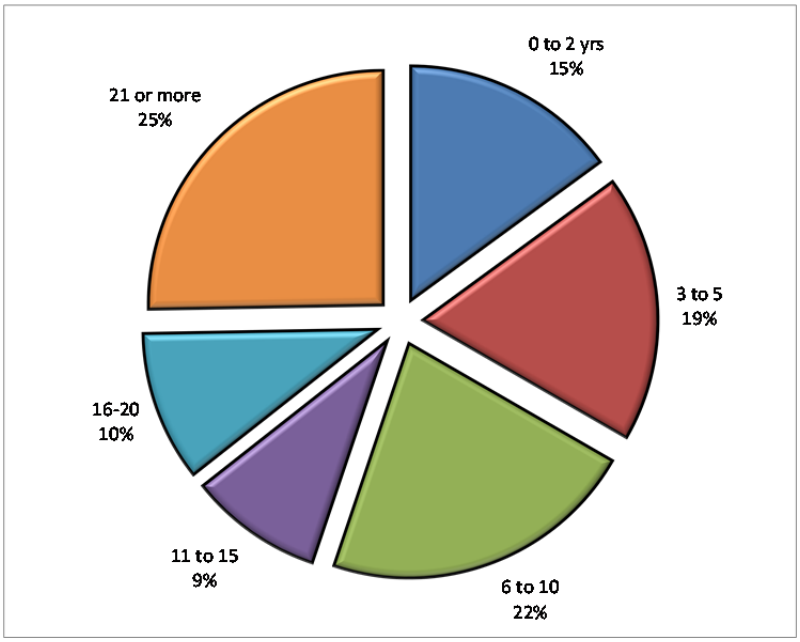

Figure 3. Breakdown of Students Participating in the Survey by Experience Level

Q5—Participants by Service

Seventy-four percent (74%) of the participants were from the Army. This is not unexpected because the survey was sent to many former SPRDE students who attended systems engineering classes at the Sterling Heights, MI, DAU campus. The Army's Tank-Automotive and Armaments Command–Life Cycle Management Command (TACOM LCMC) is located six miles from the campus and the majority of students at that location are from the Army.

The Navy participation rate was 9%, the Air Force participation rate was 7%, and the Fourth Estate[4] participation rate was 10%. Of the Fourth Estate participants, the majority were from the Defense Contract Management Agency (DCMA).

[4] "Fourth Estate" entities are all organizational entities in DOD that are not in the military departments or the combatant commands. These include the Office of the Secretary of Defense, the Joint Staff, the Office of the Inspector General of DOD, the defense agencies, and DOD field activities.

The Office of the Under Secretary of Defense for Acquisition, Technology, & Logistics (OUSD[AT&L]) publishes the number of acquisition workforce members in each of the Services. The latest report (OUSD[AT&L], 2012, p. 2) showed that the Army was 28% of the total acquisition workforce, the Navy was 35%, the Air Force was 23%, and the Fourth Estate was 14% (see Figure 4).

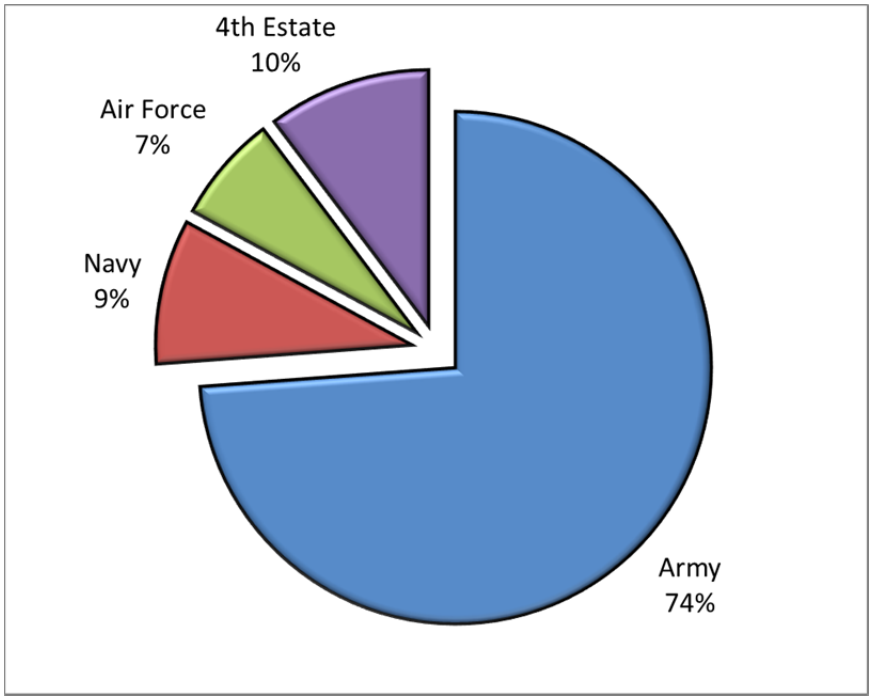

Figure 4. Breakdown of Students Participating in the Survey

Q6—Risk Management Plan

Survey Question 6 asked if the participant's organization had a documented risk management process. The purpose of this question was to determine the use of formal risk management in the participant's organization.

Only 55% answered that their organization had a documented risk management process (see Figure 5).

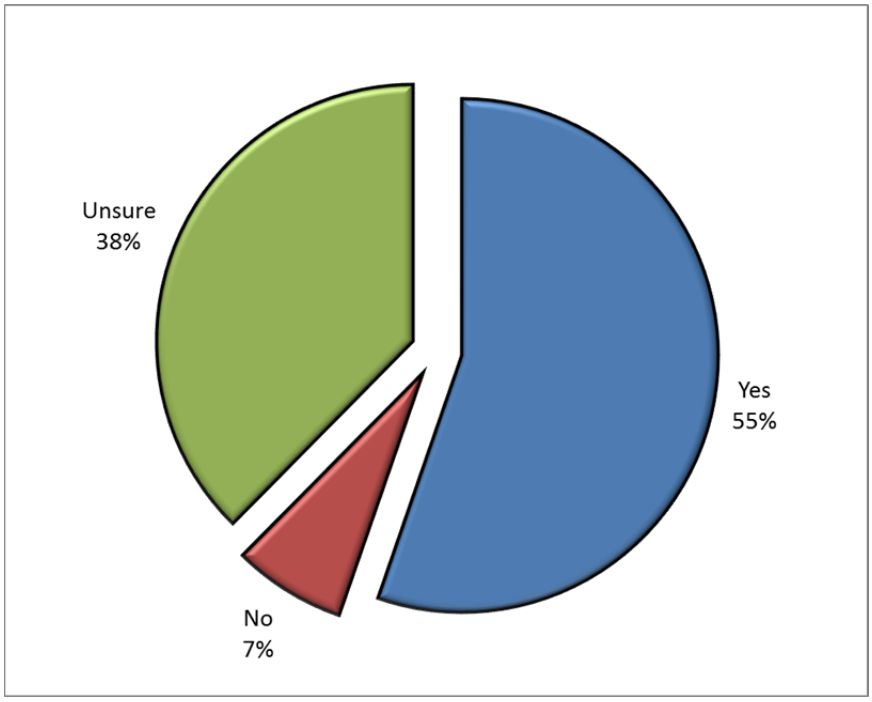

Figure 5. Number With a Documented Risk Management Plan

Q9—The Chair of a Risk Review Board

Another survey question asked if the participants knew the chair of a risk review board within their organizations. The purpose of this question was to determine the formal use of risk management in the participant's organization.

Only 25% could identify the chair, with 14% answering that the program manager (PM) was the chair of the review and 7% answering that the lead systems engineer chaired the review (see Figure 6).

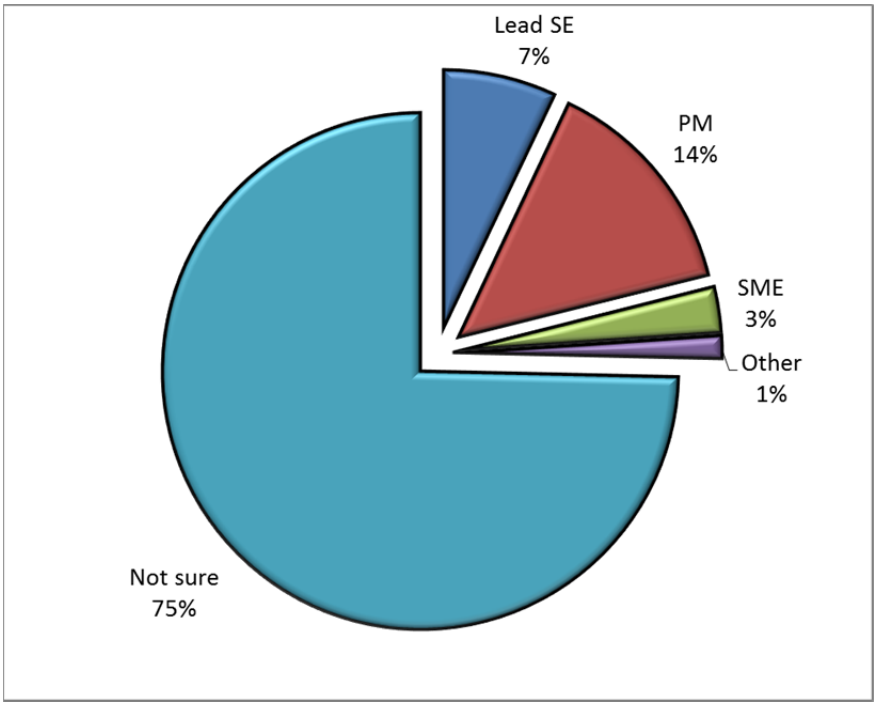

Figure 6. The Chair of the Risk Review Board

Q10—Use of a Software Tool

A survey question asked if the participant's organization used a software tool for risk management. The purpose of this question was to determine the formal use of risk management in the participant's organization.

Only 24% could identify that a software tool was in use (see Figure 7). The software tools identified were the following:

- Risk Recon (11 responses)[5];
- Excel spreadsheets (2 responses);
- ARM (Active Risk Manager; 1 response);

5 Risk Recon is an application that was developed by Program Executive Office Ground Combat Systems (PEO GCS), and the large number of responses is partially due to the relatively large number of survey participants who came from PEO GCS and other organizations at the TACOM LCMC that are using the software.

- Clearcase (1 response);
- Haztracker (1 response);
- Microsoft Access database (1 response);
- MS SharePoint (1 response);
- DOORS (1 response); and
- PM Tool (1 response).

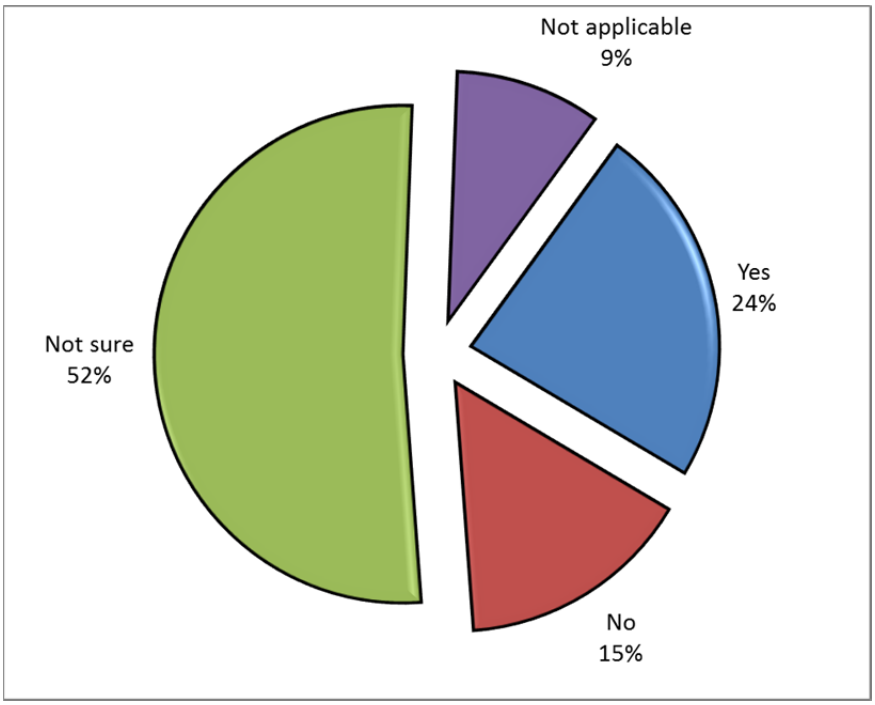

Figure 7. Software Tool

Q12—Responsibilities of the Survey Participants

A question in the survey asked the participants to identify their most important responsibilities. They could choose multiple options (see Figure 8). Systems Engineering and Program Management were the top two responsibilities with 48% and 40%, respectively.

Forty-eight percent (48%) identified one or more of the following contracting-related activities: Developing Specifications (18%); Working on RFIs, RFPs, SOWs, etc. (38%); Source Selection (13%); or Contractor Management (33%).

Requirements Generation and Developing Specifications were 20% and 18%, respectively. Design work, such as Software (5%), Hardware Design (11%), and Safety & Environment (10%) had a small number of participants.

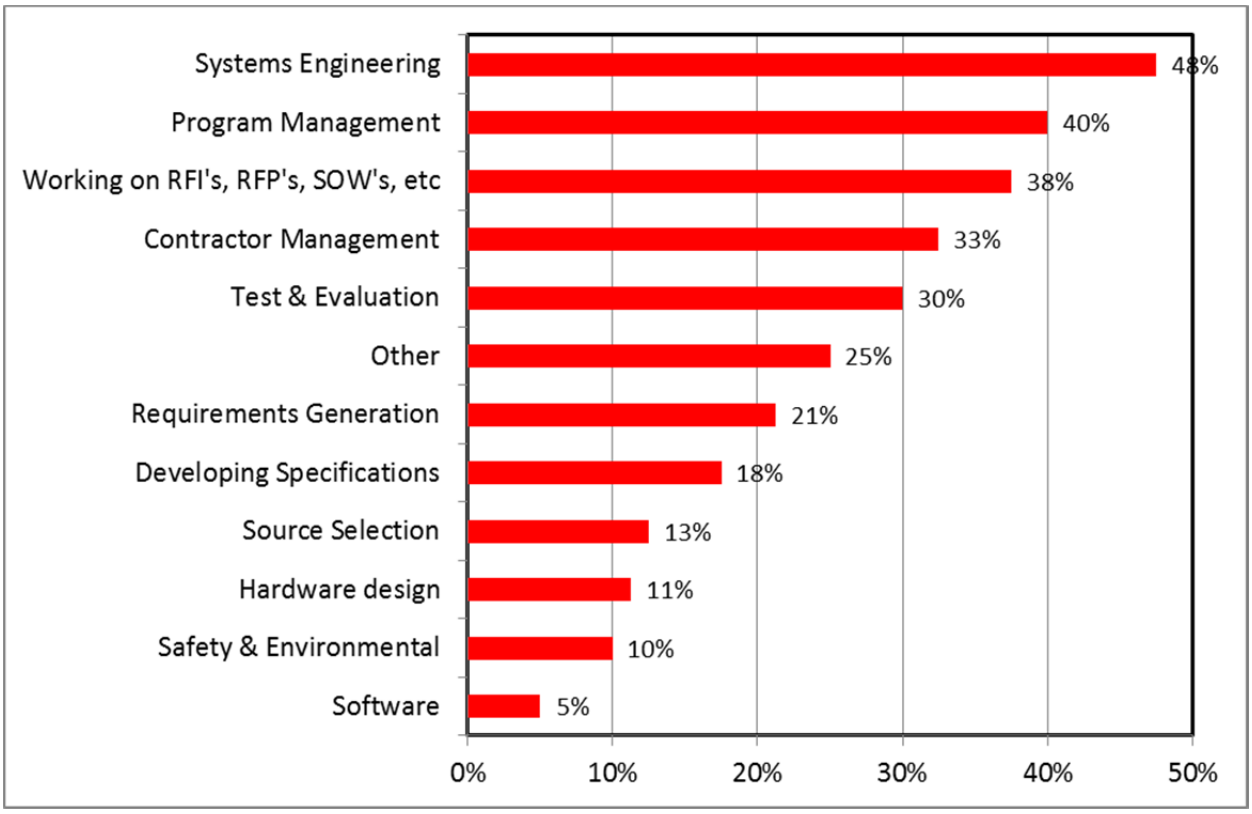

Figure 8. Key Responsibilities of the Survey Participants

Q14—Stakeholder Involvement in the Risk Management Process

This survey question was designed to identify the stakeholders involved in the risk management process. Participants were asked which of the following stakeholders they actively involved in the process of evaluating risks:

- Taxpayers,

- Congress,
- OSD,
- Users,
- PEO,
- Program office,
- System engineers,
- Testers,
- Logisticians,
- Contracting staff,
- Budgeting staff,
- Other government,
- Contractors, and
- Not applicable.

This data is from the participants' viewpoint. The actual stakeholder involvement in risk management could be different, but it was beyond the scope of this research project to survey the other stakeholders.

Figure 9 lists the responses from the participants. Fifty-four percent identified that systems engineers were involved in the risk management process. Stakeholders that were identified by 25% or more of the survey participants were users, program office, testers, contractors, contracting staff, and logistician, in that order. PEO involvement was only 15%. According to the participants, Congress did not have any direct involvement in program risk management.

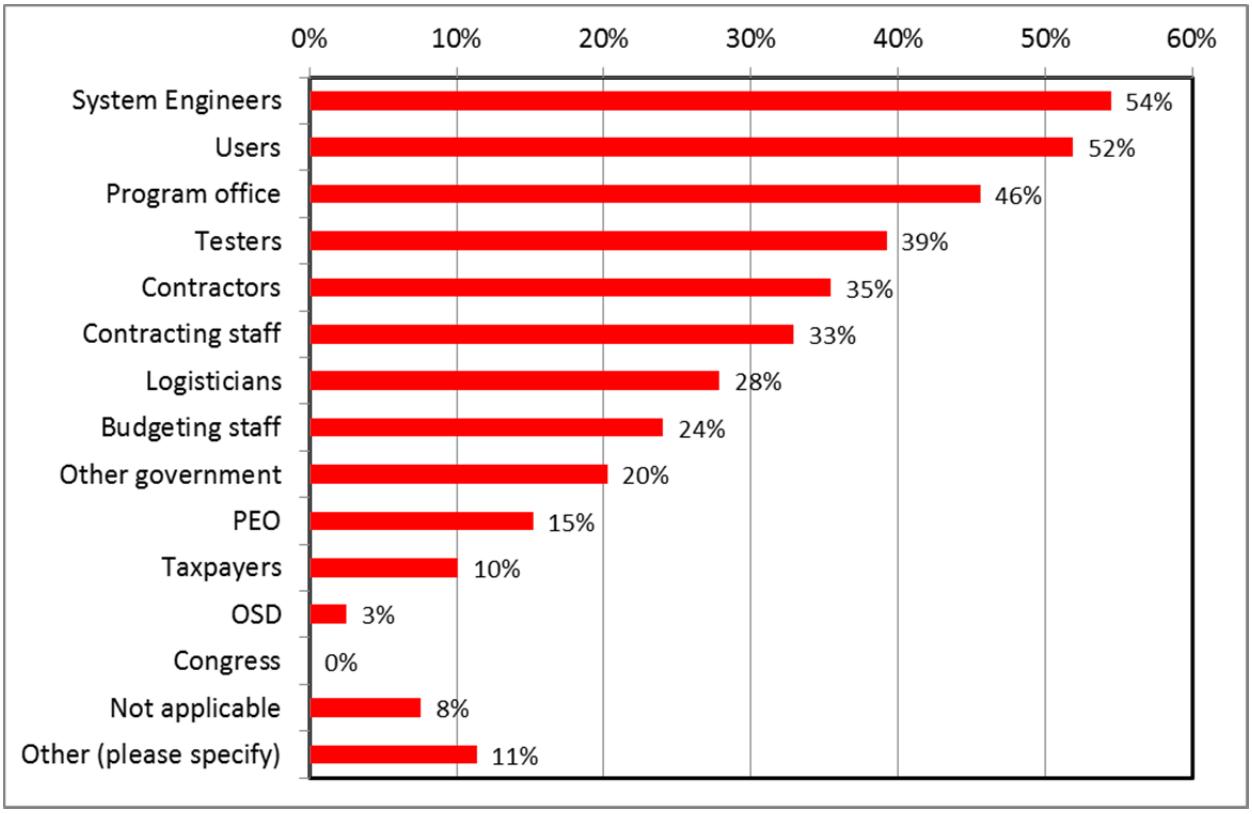

Figure 9. Stakeholder Involvement in Risk Management

Q17—Frequency of Developing a Risk Mitigation Plan

A survey question asked the participants to identify the frequency of developing risk mitigation plans within their organization. The purpose of this question was to determine the formal use of risk management and of risk mitigation in the participant's organization.

Fifteen percent (15%) identified it as "all the time" or "frequently"; 21% said "sometimes"; 23% said "never" or "seldom"; and 41% replied "not applicable," "can't quantify," or "other" (see Figure 10).

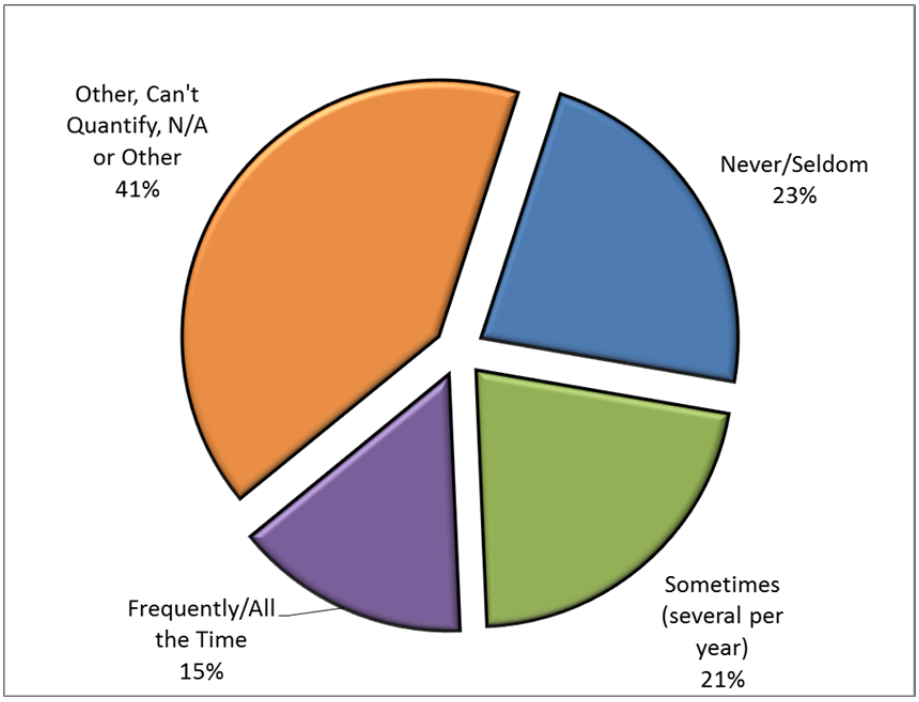

Figure 10. Frequency of Developing a Risk Mitigation Plan

Q19—The Importance of Activities for Successful Risk Management

Question 19 asked each participant what the important activities were for successful risk management. The percentages of the participants who responded "usually important" or "always important" to the responses are captured in Figure 11.

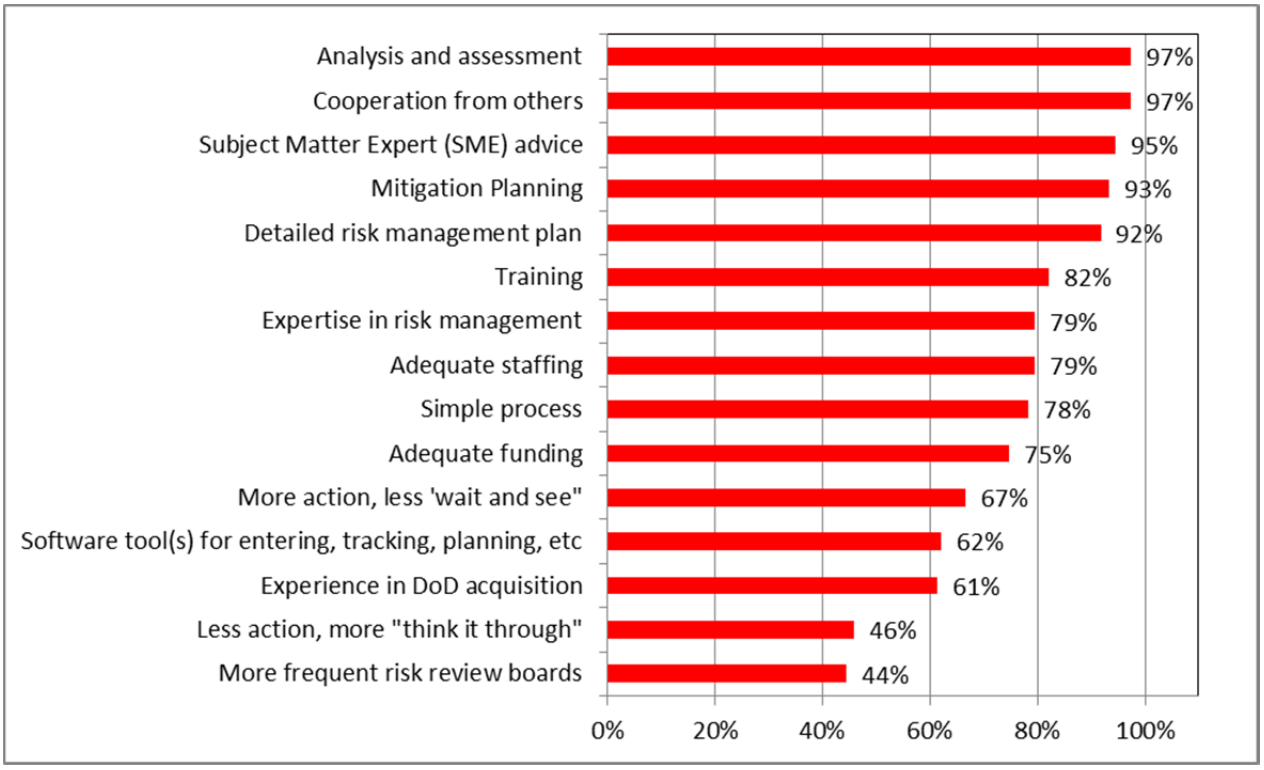

Figure 11. Important Activities for Successful Risk Management

During the analysis of the survey data, important themes emerged concerning the proficiency of doing risk management well. The top seven themes are as follows:

- analysis and assessment (97%);
- cooperation from others (97%);
- subject matter expert (SME) advice (95%);
- mitigation planning (93%);
- detailed risk management plan (92%);
- training (82%); and
- expertise in risk management (79%).

Q20—Purchasing an Extended Warranty

The purpose of Question 20 was to assess the participant's propensity to take risks in recent personal decisions. Question 20 asked participants if they purchased

an extended warranty for a recent purchase, such as a TV, appliance, smartphone, and so forth.

Thirty-one percent (31%) said that they had purchased an extended warranty while twice that number (62%) said that they hadn't. Seven percent (7%) replied "not applicable" or "unsure" (see Figure 12).

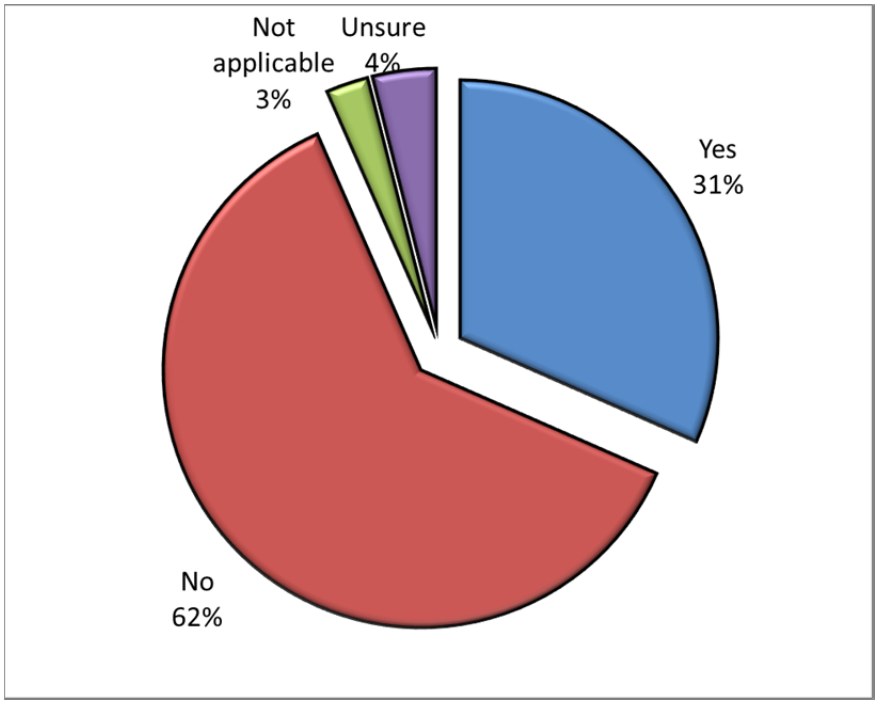

Figure 12. Purchasing an Extended Warranty

Q21—Criticality of a Warranty

Question 21 asked participants if they considered a warranty when purchasing items such as a TV, appliance, smartphone, and so forth.

Definitions of the responses are as follows:

- Critical—the buying decision was made solely based on the warranty;
- Important—an important decision factor;
- Somewhat important—aware of warranty;

- Irrelevant—not considered at all; and
- Unsure.

The warranty was a consideration in 86% of the participant replies (see Figure 13). Of those, 31% indicated it was important or critical. Only 9% said a warranty was irrelevant in their recent purchase(s).

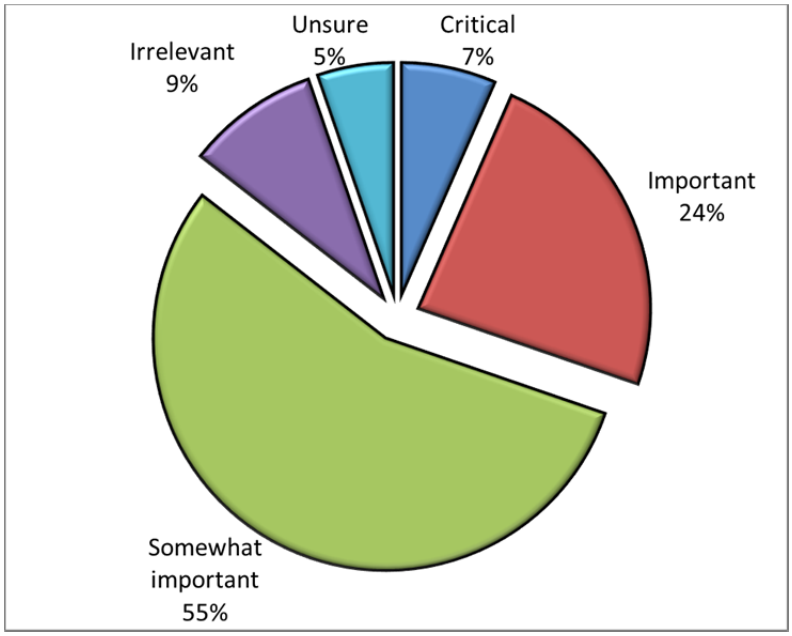

Figure 13. The Criticality of a Warranty in a Buying Decision

Q22—Decision-Making for a $500 Purchase

Question 22 measured the participant's behavior in a hypothetical purchase of a $500 item. The question was,

> If you bought a major item for $500 and could increase the warranty from 1 to 2 years, how much would you be willing to pay for the extended warranty?

There is no "right" answer to this question. If the item failed after a short period and the product maintained its value, then the value of the extended warranty could be as high as $500. However, if the product was fairly reliable, or if the value of the item dropped dramatically in a year, then the extended warranty might be nearly worthless.

However, there are other factors to consider such as (1) How will the product be used? (2) Is the person “error prone”? and (3) Will new technology make the item obsolete?

Thirty-one percent (31%) said that they would not purchase an extended warranty. Thirty-five percent (35%) replied that they would pay between $10 and $40 and 16% said that they would spend $50, which is 10% of the purchase price of the item. Fifteen percent (15%) said that they would pay between $60 and $150 (see Figure 14).

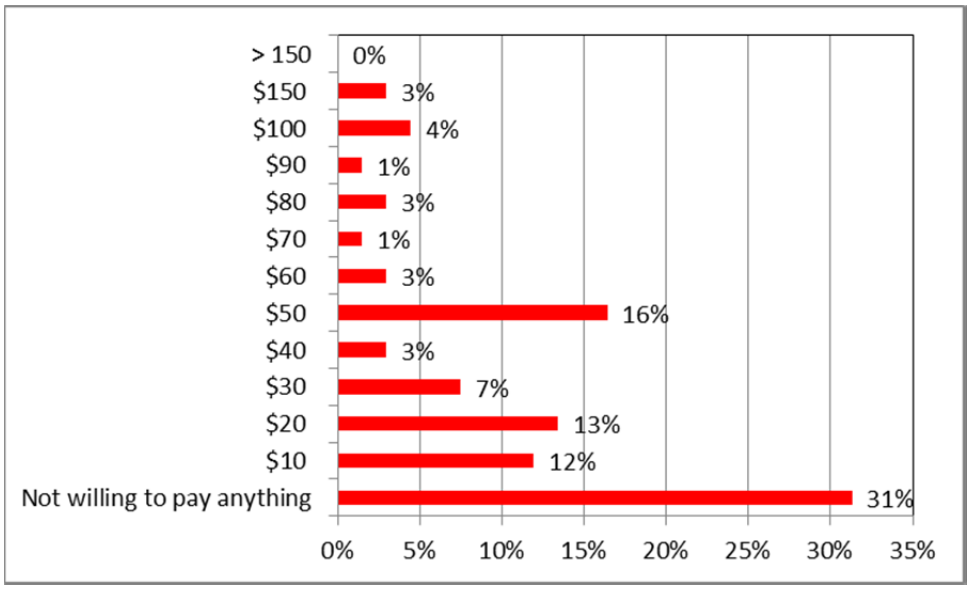

Figure 14. The Willingness to Buy an Extended Warranty in a Buying Decision

Note. The total did not sum to 100% due to rounding errors.

Q23—Willingness to Recommend Spending More This Year to Save Money in the Future

Question 23 measured the participant’s willingness to recommend spending more this year to save money in the future. The question was,

> In your current position, how likely are you to recommend and justify a budget increase this year so that costs will be lower in following years?

There is no “right” answer to this question, although the DoDI 5000.02 (OUSD[AT&L], 2008) says,

b. Consistent with this Instruction and Reference (b), the Program Manager (PM) and the MDA shall exercise discretion and prudent business judgment to structure a tailored, responsive, and innovative program. (p. 12)Thirty-one percent (31%) answered “probably” or “always,” while 18% said “possibly” (see Figure 15). Only 10% said “unlikely” or “never.” However, 29% said “not applicable,” and 11% said “other.” The following are a couple of the interesting “other” responses:

> I do R&D. We can do more research and development … with more money. So I’m always able to justify a budget increase. With less money we do less work, and have less systems available when the time comes for improvements in the area I work. We just implement and correct later if the budgets are too low.

The second response was,

> Unlikely because I don’t believe the costs will actually be lower in the following years. I think there will be some change that was “unforeseen” that will require additional life-cycle costs. If the future savings was guaranteed, I’d always spend the money now.

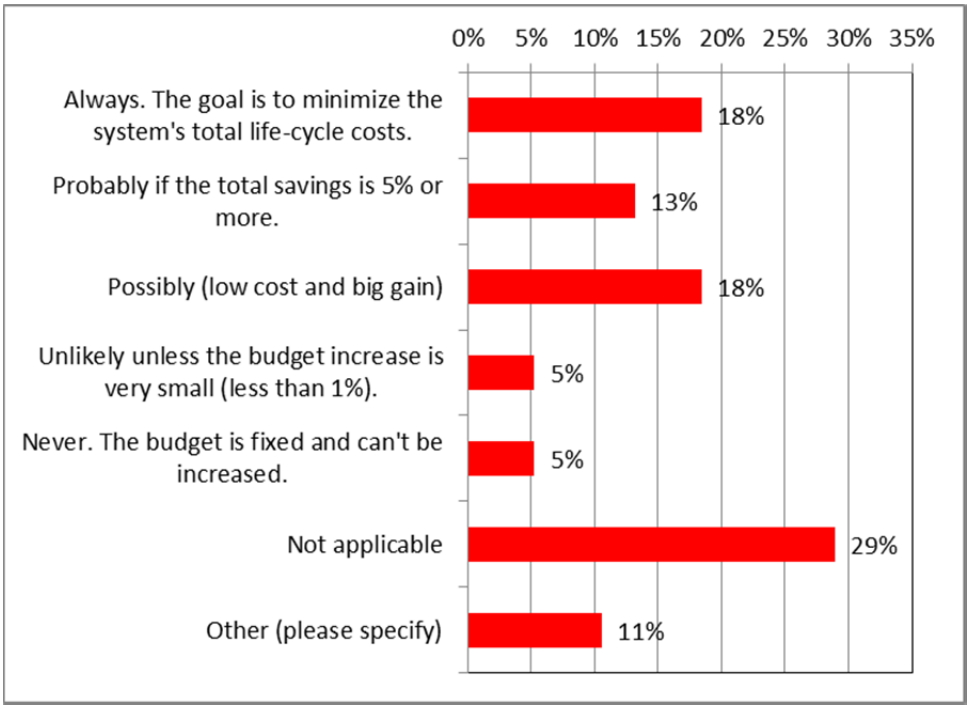

Figure 15. The Willingness to Recommend Spending More This Year to Save Money in the Future

Note. The total did not sum to 100% due to rounding errors.

Q24—Willingness of the PM to Recommend and Justify a Budget Increase This Year so That Costs Will Be Lower in Following Years

This question focused on the actions of the program manager. Question 24 measured the participant's belief that the PM (or other program leader) would recommend spending more this year to save money in the future. The question was,

> How likely is the manager (PM or other) to recommend and justify a budget increase this year so that costs will be lower in following years?

Forty-five percent (45%) of the respondents said that the PM was "possibly," "likely," or "always" going to recommend a budget increase. Only 18% said the PM was "unlikely" or "never" going to recommend a budget increase. Thirty-five percent (35%) replied "not applicable" or "other".

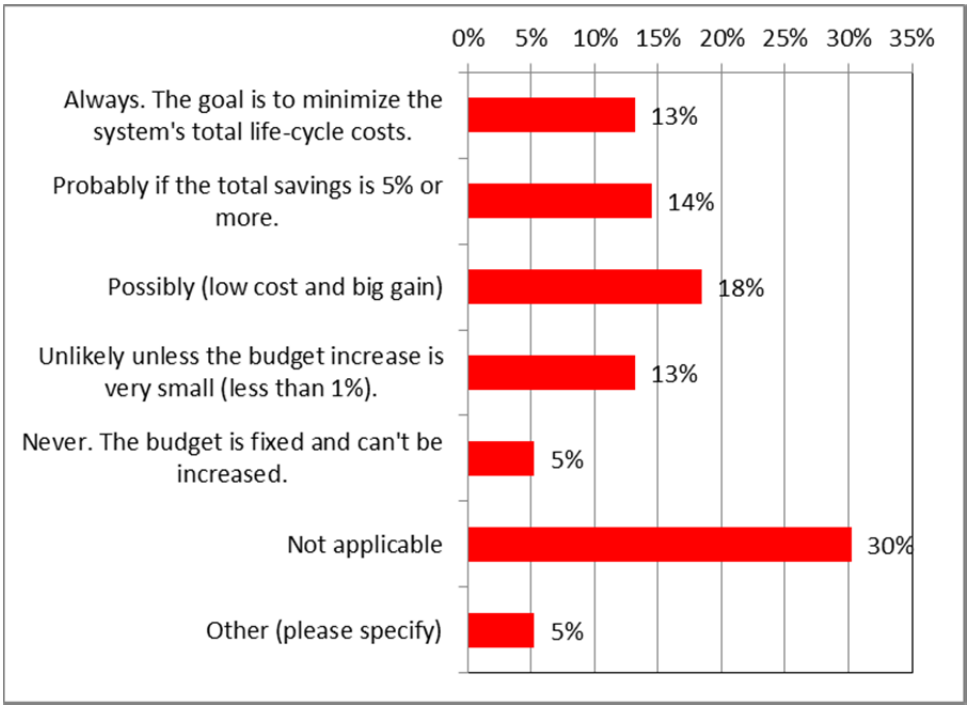

Figure 16. The Willingness of the PM To Justify a Budget Increase This Year to Save Money in the Future

Note. The total did not sum to 100% due to rounding errors.

Q25—Willingness to Spend Money on Risk Mitigation

This question focused on the actions of the individual. Question 25 measured the participant's willingness to spend money on risk mitigation activities. The question was,

> There is a 50% chance that a test next year will fail. Redoing the test will cost $10,000. How much would you recommend the PM to spend this year to reduce the likely failure rate next year to 10%?

There is no "right" answer to this question. The expected loss[6] without any mitigation is $5000 (50% x $10,000), and the expected cost savings if mitigation efforts are successful is $4000 (40% x $10,000). However, even though the

[6] The expected loss of a risk element is the average consequence (loss) that would occur if the risk item was encountered multiple times in similar circumstances.

likelihood and consequence were given, in real situations they are usually estimates which can have a large degree of uncertainty.

The respondents' replies ranged from zero to $10,000 (see Figure 17). Half (51%) said they were willing to spend up to $4000, the expected savings. However, 29% recommended spending over $4000, and 8% even recommended spending $10,000, the total possible loss. Twelve percent (12%) replied "other" or "not sure".

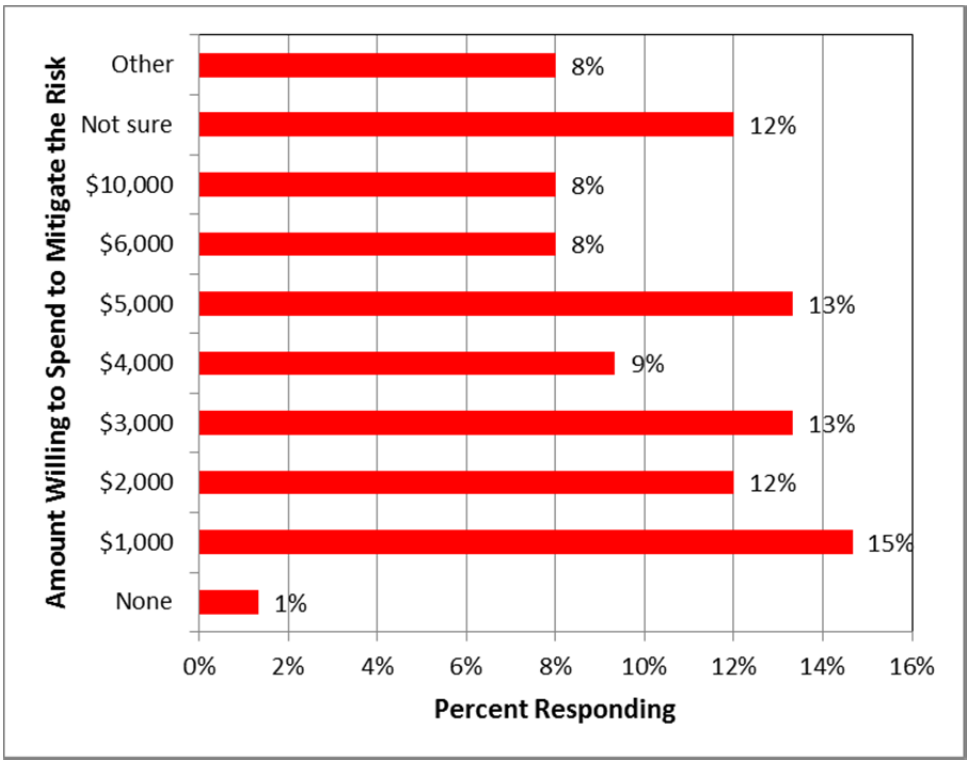

Figure 17. The Willingness to Pay for Risk Mitigation Activities

Note. The total did not sum to 100% due to rounding errors.

Q26—Expectation of Fulfilling Work Commitments

Question 26 is very similar to Question 25, but this time the scenario is that the respondent is solely responsible for the possible cost increase. The question was,

> The results of the tests will influence your appraisal next year. There is a 50% chance that YOUR test next year will fail. Redoing the test will cost $10,000.

How much would you recommend the PM to spend this year to reduce the likely failure rate to 10%?

There is no "right" answer to this question. The expected loss without any mitigation is $5000 (50% x $10,000), and the expected cost savings if mitigation efforts are successful is $4000 (40% x $10,000).

The respondents' replies ranged from zero to $10,000 (see Figure 18). A little under half (47%) said they were willing to spend up to $4000, the expected savings. However, 39% recommended spending over $4000, and 13% even recommended spending $10,000, the total possible loss 50% of the time.

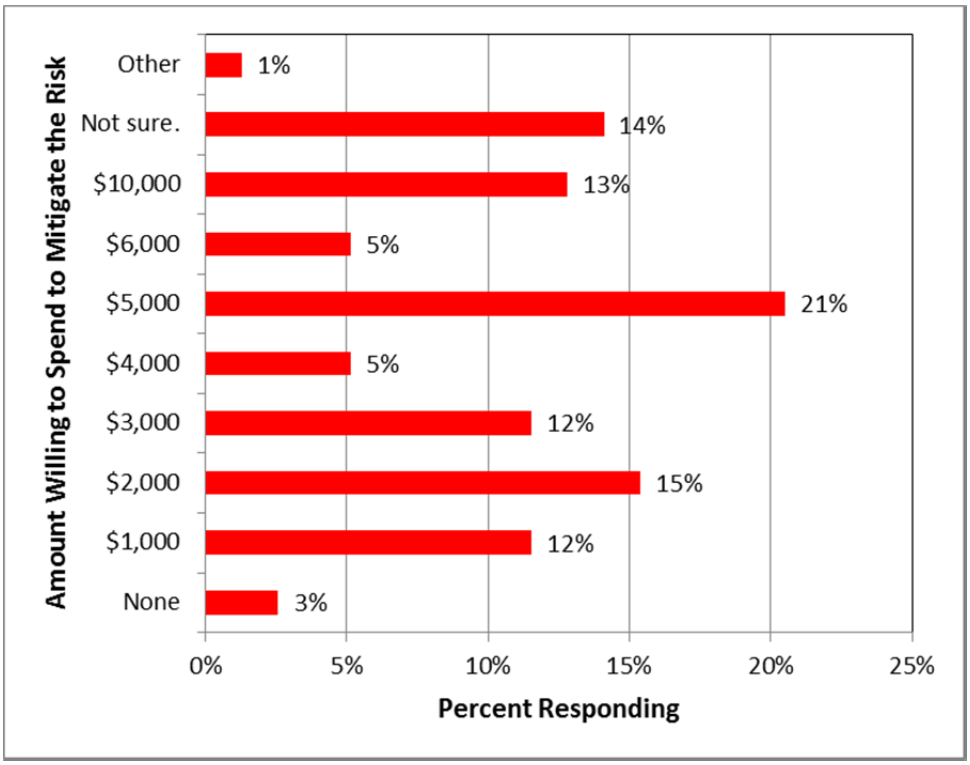

Figure 18. The Willingness to Pay for Risk Mitigation Activities—Task 1

Note. The total did not sum to 100% due to rounding errors.

Q27—Another Example of the Expectation of Fulfilling Work Commitments

Question 27 is very similar to Question 26, but this time the scenario is that it is another government entity that is responsible for completing the work. The question was,

> A DoD research lab has agreed to develop a new and important software application for your program. They are working under a MIPR. They estimated that it would take 10 months to complete at a cost of $100,000. But a SME who was asked to comment on the project said she believes that there is a 20% chance that it will take 12 months and cost $120,000. How much extra are you willing to pay the DoD research lab up front so that the software can be completed on time?

There is no "right" answer to this question. The expected cost overrun is $5000 (20% x $20,000).

The respondents' replies ranged from zero to $20,000 (see Figure 19). A little under half (48%) said they were willing to spend up to $5000, a little more than the expected savings.[7] This value is the same as the response to the previous question. Twenty-one percent (21%) recommended spending over $5000, and 12% even recommended spending $20,000, the total possible loss.

[7] The survey responses were poorly chosen. The value of $4000 should have been a possible response for the participant.

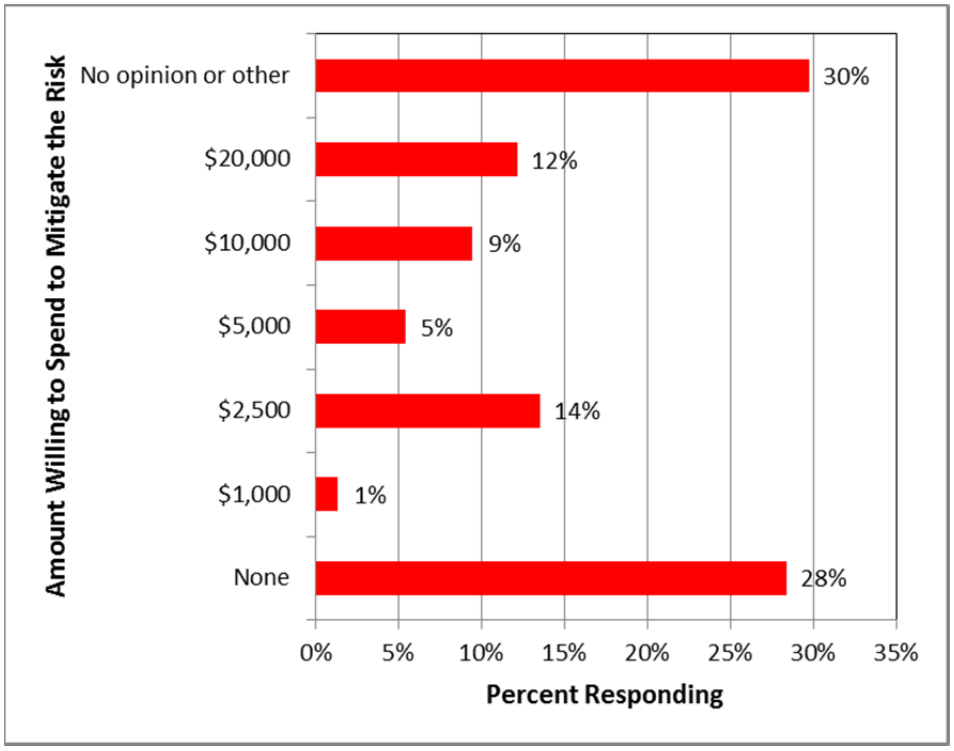

Figure 19. The Willingness to Pay for Risk Mitigation Activities—Task 2

Note. The total did not sum to 100% due to rounding errors.

The following are some comments from participants[8]:

- Depends on the justification of the 20% whether it is best on [sic] "expert opinion" or whether it is based on objective evidence.
- Depends upon the consequences of slipping schedule and the possible cost of same.
- Establish a reserve fund with 10% of the budget in anticipation of schedule/cost increases.
- Goverment [sic] labs will constantly perform behind schedule and over budget. Thus, I'd recommend funding them for 9 months and $90k. Assume they'll come back and ask for more funding which can then be doled out in 1 month incriments [sic]. For the funding profile described,

[8]Comments provided in the "other" category that were the same as one of the standard responses were counted as part of the standard responses.

it's only a half-person working on the project. Best way to increase producrivity [sic] and minimize risk would be to fund at the $20k/month level to have full-time staff assigned to the project.

- I would open a dialog with them to try to identify causes to reduce the cost/schedule risk, rather than just offering them money up front. How much I'd be willing to pay depends on other factors not described here (how important the cost/schedule factors are).
- I would take the SME comments to the DoD research lab and compare notes with the people who made the 10 month commitment at $100K. If they were to agree with the comments I would consider making a change to the cost and timing.
- It depends on the scheduling requirement for fielding
- Need to get feedback from SME what possible mitigations are prior to paying extra. If the reason for the additional money cannot be clarified it could be a number of possible indications including a need to cancel the project depending on the fidelity of the answer.
- They'll come asking for the money later anyway, don't front load the money.

Q28—A Third Example of the Expectation of Fulfilling Work Commitments

Question 28 was not written very clearly so the responses will not be analyzed in this research report.

Q29—Recommendations for Improving Risk Management in the DoD

Question 29 was the last question of the survey and asked the participants to give their recommendations for improving risk management within the DoD. Participants were allowed to give multiple responses.

There were six major themes in the participants' recommendations (see Figure 20). The responses have been summarized below into six themes. While the responses are considered very valuable, the data set is not large enough to call these recommendations "best practices," since that would imply that multiple

organizations are doing similar activities and are seeing similar outcomes from the practices.

The six themes are as follows:

1. standardized tools and processes (36%);
2. training (21%);
3. leadership (management guidance; 13%);
4. change in organizational culture (11%);
5. general systems engineering activities (11%); and
6. budgeting issues (8%).

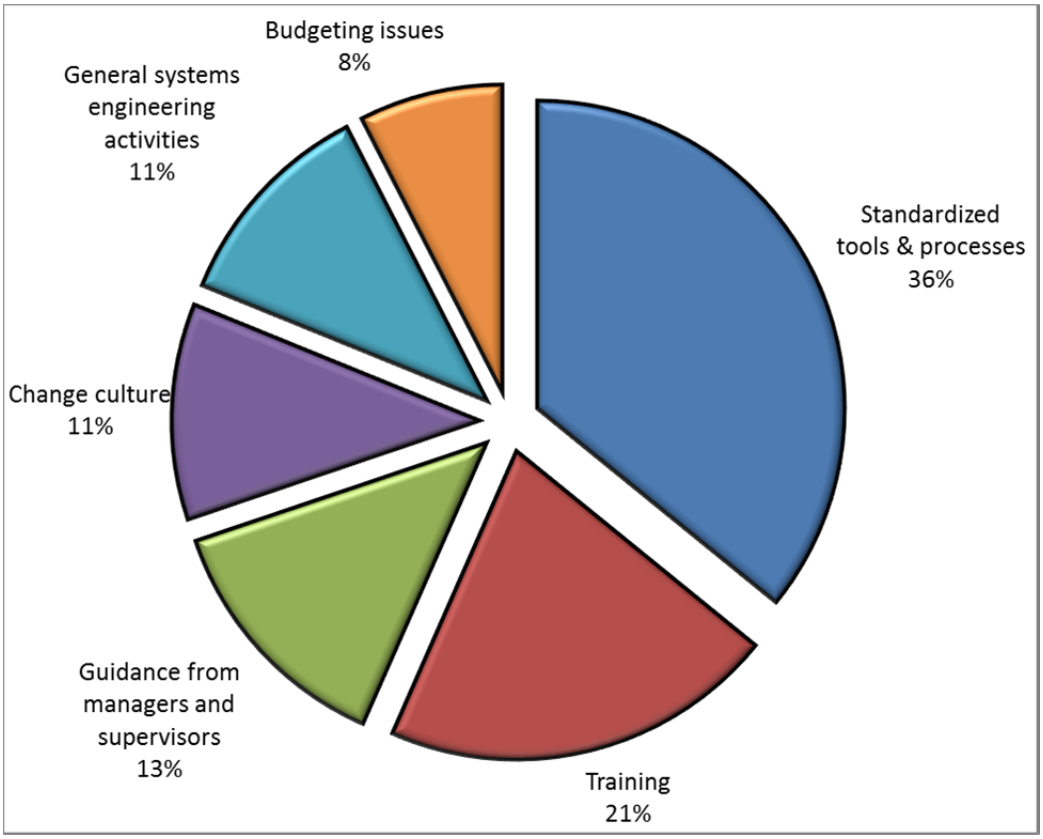

Figure 20. Participant Recommendations Classified by One of the Six Theme Areas

Standardized Tools and Processes (36%)

The biggest group of recommendations (36%) for improving risk management practices in the DoD was in standardized software tools, standard processes, and other activities related to performing risk management. An important recommendation is a data repository to aid in quantifying likelihood and consequence and to aid in the development of risk mitigation plans. This category also includes analysis and failure-mode and effects analysis (FMEA). Another recommendation is the use of Subject Matter Experts (SMEs), which is already a best practice.

Training (21%)

Twenty-one percent (21%) of the recommendations involved training. Participant comments included mandatory training for everyone at all levels, interactive training, subcontractor training, PM training, training of people new to risk management, and cross-training.

Leadership (Management Guidance) (13%)

Thirteen percent (13%) of the recommendations can be classified as leadership issues. Recommendations mentioned by participants included better guidance and better teaming.

Change Culture (11%)

Eleven percent (11%) of the participants' recommendations had to do with the culture of the organization. Suggestions included empowerment, better teaming, a culture of always doing risk management, more critical thinking, and more decisiveness. Some of these recommendations could also fall under Leadership.

General Systems Engineering Activities (11%)

While risk management is part of systems engineering, general systems engineering practices exclusive of risk management were recommended (11% of total). Comments on systems engineering included early planning, more emphasis on quality, and more life-cycle analysis.

Funding (8%)

Eight percent (8%) of the recommendations dealt with funding issues. Comments included the culture of limitless funding, better program funding, and more incentives for contractors to meet cost and schedule objectives.

V. Conclusions and Recommendations

There are several conclusions and recommendations based on this research project.

A. Utilization of Risk

Question 6 showed that only 55% of the participants knew of a risk management plan for their organization. Question 9 showed that 75% were unsure of the chair of a risk review board in their organization. Question 10 showed that only 24% knew of a software tool being used by their organization.

The data show the need for more effective risk management. DoD programs are inherently risky. The DoD is not going to develop a new program unless the system is needed to replace an existing system or unless a new system is developed to fill an identified capability gap. In both cases, the system will employ new and advanced technologies. (There's no reason to develop a system that is a little better than the previous system.)

Tom DeMarco (2002) identified three core risks that he had observed on all projects. First, there was the risk of "function inflation" (i.e., requirements creep). Changing requirements was costly, delayed completion of the project, and could impact the performance of the system in some areas while new requirements were implemented.

The second risk that DeMarco identified was specification breakdown. That is, the stakeholders couldn't agree on what the project would do. He said that this risk was almost always fatal to the program.

The third core risk was under-sizing the effort, which resulted in a cost estimate that was too low. Thus, there would be a cost overrun even if the program was executed well.

Two other important risks for DoD programs are funding (type of funds, total amount, and yearly amounts) and technology utilization. Funding is a risk because of the before-mentioned low cost estimates, costly new requirements, changes in DoD priorities, and program delays that result in the wrong type of money for the fiscal year. Technology is a risk because DoD programs will always assume high technical risk. The DoD is not going to spend millions or billions of dollars on a program that is a little better than an existing system. Technology will almost always be used to enable the performance gains or cost reductions planned.

There is no point in saying that better risk management is required. That's obvious. Nor does it make sense to say that the DoD leadership needs to push for better risk management. Risk management is a requirement of the DoDI 5000.02 (OUSD[AT&L], 2008), the DoD has developed a risk management guidebook (DoD, 2006), risk management is presented in the DoD *Acquisition Guidebook* (DoD, 2012), and risk management is taught in many DAU classes.

A starting point is to have all programs address the five core risks: requirements creep, unclear program objectives, low cost estimates, funding problems, and the use of new technology. These should be standard risk topics. That is, they should be reported for all programs at every review meeting. It is likely that when a program office addresses these five core risks, other areas of risk will also be identified, analyzed, and mitigated.

B. Importance of Activities

Question 19 identified the most important activities required for successful risk management. The top seven activities are directly or indirectly related to the effectiveness of doing risk management. The activities identified by the participants include

- analysis and assessment (97%);
- cooperation from others (97%);

- subject matter expert (SME) advice (95%);
- mitigation planning (93%);
- detailed risk management plan (92%);
- training (82%); and
- expertise in risk management (79%).

C. Training

The participants identified six important activities required for performing effective risk management. It is not sufficient to provide the acquisition workforce with basic training on likelihood, consequence, mitigation, and so forth. The training must develop

- skills to identify, analyze, and assess risks;
- the role of teaming and the integrated product and process development (IPPD) philosophy;
- detailed risk processes and plans (at some level, this will be unique to the organization); and
- expertise in risk management via mentoring, SMEs, and data repositories.

The principles of risk management are taught in most DAU classes, but the answers to Questions 25, 26, and 27 show that additional training is needed on the concepts of likelihood, consequence, and expected value.

Furthermore, the results of Question 12 indicate that 48% of the survey participants had responsibilities in some area of contract management (the categories were developing specifications; working on RFIs, RFPs, SOWs, etc.; source selection; or contractor management). The contracting responsibilities listed by the survey participants are covered in ACQ-201, SYS-203, and SYS-302, although any enhancements in training in this area would benefit an estimated 48% of the workforce.

D. Repository of Data

Making effective risk management decisions requires good data. SMEs will provide much needed experience, but a risk repository needs to be developed at the program, PEO, and Service level to enable data-based decisions. Creating a repository will take discipline since the value of the repository won't be realized for many months, if not years.

E. Culture Change

The participants identified various aspects of "organizational culture" that need to change, including empowerment, better teaming, a culture of always doing risk management, more critical thinking, and more decisiveness. Changing the culture of an organization usually takes many years, dedication from leadership, and acceptance by the workforce.

F. Analyzing Risks

Questions 25, 26, and 27 all dealt with a scenario requiring a decision about the level of mitigation to implement (in this case, money). There are no right answers to these scenarios. A decision should be based on factors such as the product price, failure rate, likelihood of obsolescence, new technology, criticality to the mission, and so forth.

However, it is important to note that there was a wide variation in answers, from "no investment" in mitigation to an investment equal to the total value of the product or service. That is, there was no consistency in deciding on the risk mitigation plan. More effective risk management training will better enable the workforce to make data-driven decisions regarding risk mitigation.

List of References

Barkley, B. T. (2004). *Project risk management.* New York, NY: McGraw-Hill.

Blanchard, B. S., & Fabrycky, W. J. (2011). *Systems engineering and analysis.* Boston, MA: Prentice-Hall.

Charette, R. N. (1989). *Software engineering risk analysis and management.* New York, NY: Intertext Publications/Multiscience Press.

Department of Defense (DoD). (2012). *Defense acquisition guidebook* (Ver 1-November-2012). Retrieved from https://dag.dau.mil/pages

Department of Defense (DoD). (2006). *Risk management guide for DoD acquisition* (6th ed.). Washington, DC: Author.

Grey, S. (1995). *Practical risk assessment for project management.* ChicWest Sussex, England: John Wiley & Sons.

Office of the Under Secretary of Defense for Acquisition, Technology, & Logistics (OUSD[AT&L]). (2008). *Operation of the defense acquisition system* (DoD Instruction 5000.02). Washington, DC: Author.

Office of the Under Secretary of Defense for Acquisition, Technology, & Logistics (OUSD[AT&L]). (2012). *FY12(Q2) defense acquisition workforce count matrix (by components/careers).* Washington DC: Author.

Rowe, W. D. (1977). *An anatomy of risk.* New York, NY: John Wiley & Sons.

Vose, D. (2008). *Risk analysis: A quantitative guide* (3rd ed.). Chippenham, Wiltshire, Great Britain: John Wiley & Sons.

THIS PAGE INTENTIONALLY LEFT BLANK

Appendix A. Survey Questions

2 What Defense Acquisition Career Field are you in?

3 How many total years of professional experience do you have, specifically, in the military, as a government civilian or in private industry?

4 How many years have you worked for the U.S. government (in the military and/or as a civilian)?

5 What is your service affiliation?

6 Does your organization have a documented risk management process?

7 If your organization has a risk management plan, when was the last time you reviewed it?

8 Does your organization hold risk review boards?

9 If your organization holds a Risk Review Board, who chairs it?

10 Does your organization use a software tool for managing the risk management process?

11 If you answered Yes to the previous question, what is the name of the software application used to manage the risk management process in your organization?

12 What are some of your key job responsibilities? (You may select more than one)

- o Program management
- o Systems engineering
- o Hardware design
- o Software design
- o Test and evaluation
- o Safety, Environmental
- o Requirements generation
- o Developing Specifications
- o Working on RFI's, RFP's, SOW's, etc.

- o Source Selection
- o Contractor management
- o Other If you answered other, please provide a short description of your responsibilities (one per line)

13 On average, how often do you factor risk into your decisions?

14 When evaluating risks, which of the following stakeholders do you actively involve in the process? (select all that apply)

- o Taxpayers
- o Congress
- o OSD
- o Users
- o PEO
- o Program office
- o System Engineers
- o Testers
- o Logisticians
- o Contracting staff
- o Budgeting staff
- o Other government
- o Contractors
- o Not applicable
- o Other (please specify)

15 When evaluating risks, if there is a conflict in stakeholder requirements, what steps do you take to resolve those conflicts? (You can select more than one)

- o Not applicable
- o Ask for a peer to intervene
- o Ask for a SME to intervene
- o Discussion then a unilateral decision (one person making the decision)
- o Discussion then a consensus decision (group decision)
- o Get higher authority to make a decision
- o Not sure
- o Other (please specify)

16 Do you prepare risk mitigation plans for medium or high risks?

17 How often do you develop a mitigation plan for a medium or high risk?

18 How much of your typical day is spent on risk identification, assessment, developing a mitigation plan and/or monitoring mitigations actions?

19 In your opinion, how important are the following activities for successful risk management?

- o Detailed risk management plan
- o Simple process
- o Training
- o Software tool(s) for entering, tracking, planning, etc.
- o Adequate funding
- o Adequate staffing
- o Expertise in risk management
- o Experience in DoD acquisition
- o Cooperation from others
- o More frequent risk review boards
- o More action, less 'wait and see"
- o Less action, more "think it through"
- o Analysis and assessment
- o Mitigation Planning
- o Subject Matter Expert (SME) advice

20 When you last purchased a major item (like a TV, appliance, smart phone, etc.), did you purchase an extended warranty?

21 When you buy a major item (TV, appliance, smart phone, etc.), how important is the product warranty?

22 If you bought a major item for $500 and could increase the warranty from 1 to 2 years, how much would you willing to pay for the extended warranty? (Pick the answer closest to your reply)

23 In your current position, how likely are you to recommend and justify a budget increase this year so that costs will be lower in following years?

24 This is a similar question to the previous question, except this one is for the manager (or PM). How likely is the manager (PM or other) to

recommend and justify a budget increase this year so that costs will be lower in following years?

25 There is a 50% chance that a test next year will fail. Redoing the test will cost $10,000. How much would you recommend the PM to spend this year to reduce the likely failure rate next year to 10%?

26 This is a similar question to the previous question, but in this case you are solely responsible for the success or failure of the test next year. The results of the tests will influence your appraisal next year. There is a 50% chance that YOUR test next year will fail. Redoing the test will cost $10,000. How much would you recommend the PM to spend this year to reduce the likely failure rate to 10%?

27 A DoD research lab has agreed to develop a new and important software application for your program. They are working under a MIPR. They estimated that it would take 10 months to complete at a cost of $100,000. But a SME who was asked to comment on the project said she believes that there is a 20% chance that it will take 12 months and cost $120,000. How much extra are you willing to pay the DoD research lab up front so that the software can be completed on time?

28 This is somewhat similar to the previous question. A DoD research lab has agreed to develop a new and important software application for your program. They are working under a MIPR. They estimated that it would take 10 months to complete at a cost of $100,000. But a SME who was asked to comment on the project said she believes that there is a 20% chance that additional training up front could shorten the development time by 2 months and reduce the costs by $20,000. How much extra are you willing to pay the DoD research lab up front so that they can complete the job 2 months early?

29 What are your recommendations for improving risk management in the DoD?

Appendix B. Answers to the Open-Ended Question on Recommendations for Improving Risk Management

Question 29 was the last question of the survey and asked the participant to give their recommendations for improving risk management within the DoD. The recommendations were summarized in Chapter 4 but are listed in their entirety below.

- Stop the culture of limitless sources of money for the "military industrial complex."
- Be more critical and challenging
- Manditory [sic] training on risk management in increase the understanding of what risk management does and how it will improve DOD operations. This training should be done at all levels so there is no confusion at any level of what it means.
- Reward decisiveness. too much indecision.
- Early identification, bringing SME, good plan
- Change to a culture of quality. Train, check report. Make quality a stronger player on all decisions. Make the quality manager the PM's right-hand-man...
- I have none at this time, as I do not have very much involvement [sic]/experience in risk management [sic].
- Provide a standard for Risk Management in a form of a DoD Directive that is available for all to follow.
- Interesting survey.
- Keep things simple and maybe have more direct guidance, like a repository of real life examples.
- More involvement from all groups. More explaination [sic] on the purpose of the reviews.
- Standardize methods, software, reviews, and implement training.

- Need a common risk matrix that is tailorable [sic] to all events. This has been developed by Mr. Don Swallom (Army Civilian) and presented at System Safety Society conference in 2011.
- Unsure since being an intern and new to the government, I have not dealt with risk management. I do not have any experience with risk management thus my recommendation would be irrelevant.
- Train PMs that technical risk is part of pushing the envelope. Having fall-back positions is good. At the end of the day, we'll have better performing systems if we allow engineers/scientists to push the boundaries of physics. This will minimize long term cost by requiring fewer future tech refreshes.
- Plan a budget to use to help mitigate risk.
- Transform the culture of DoD from doing risk management because it is required to doing risk management because it will aid the program to meet its goals.
- I would do a better job of focusing the goals of all the DoD organizations to work to the same end goal. I would also recommend that there be more sharing between teams and organizations. If everyone works to different goals we will always spend too much money, and never get to our overall goals - Being the worlds most advanced fighting force and cost appropriate at the same time.
- Additional training and standardized risk management tools
- Choose programs to be funded more carefully. Avoid funding programs that are irrelevant and don't promote competition amongst companies of all sizes and types. Fund more development work and less sustaiment [sic] and production work. This funding source provides the most stimulus to the company secor [sic] and inadvertently [sic] raises revenue for the government based on tax the same companies that were financially funded.
- N/A
- Training for those who are new to Risk management would be a nice way to introduce them to the process. I know of a few people who have just been thrown into a Risk IPT before, yet they had no idea what to expect. It was a bad experience for them.

- With very little DoD experience, I am speaking from my industry background - standardization of tools and processes - allowing for tailoring to simplify as necessary or justified.

- Have some mandatory training that is very interactive

- Offer extensive training concerning the identification and mitigation of failure and risk. Teach that significant savings are realized when steps are taken to find and mitigate risk and failure; we can “do it right the first time!” Mandate the use of FMEA (Failure Mode and Effects Analysis) so that all forms of risk and potential failure are identified. Choose risks to mitigate based on their level of risk priority (combined product of severity, occurrence, and detection) and address the pareto of higher level risks knowing that this will give the greatest return on investment. Use Risk Recon or other risk management tools to manage the mitigation actions.

- The biggest opsticle[sic] is proper guidance. Risk management controls developed for government agencies are difficult to apply to the tactical enviroment [sic] and are challenging to implement. Many Certifying Athorities [sic] or Rick Management Professionals lack the experiance [sic] in Risk Management and don’t often understand the impact on the user or the organization. Other very important factors are: Awareness, Management Support, Proper Funding, Proper Tools, and Educated Proffesinals [sic].

- More cross-training and better understanding of secondary and tertiary effects. Better prioritization and definition of requirements and critical items (cost vs. schedule vs. performance). Standardized tools for decision-making, so that decisions are not made based on the PM’s whim.

- Formal methods. I think the red-tape is a huge barrier in DoD for improving any process. Incentives for reducing cost/schedule seem to work in private industry. Empowerment, in my opinion, managers DoD-wide are helpless when it comes to correcting/removing people who refuse to support new approaches such as risk management.

- Need to gt [sic] a bit more familiar as a whole. It has been a long time since I was in a position that required a strong inherent interest in RM.

- Change of culture. Guidance from managers/supervisors down to lower levels that it is okay (and necessary) to take reasonable risks, if it means chances are good to save over the long term.

- Don’t get me started. I think there are lots of things within the Army that need to be improved upon or brought up-to-date. I have more experience in the IT portion than the risk management sector. From what I’ve seen, however, I would recommend that testing and validation criteria be brought up-to-date, that IT and IA staff are trained, that better and automated processes be utilized, and that pencil-whipping cease. I recommend true evalations [sic] of risk against meaninful [sic] criteria. I recommend those responsible for implementing changes to improve security posture take their role seriously and recommend that they stop trying to pull an Obewan Kenobee on us (“the risk you see is not truly a CAT-I; it does not exist”) and actual identify the risk for what it is and address it accordingly. Good luck, Don! John K. Weaver
- I believe training and mentoring is the key to improve the process.
- More management emphasis on importance of risk management
- I’m not for sure. I do not deal with risk management personally so I do not know what’s being done or what is not.
- none
- More specific examples from real life hit and miss situations.
- Risk has to be identified early in project. SMEs are very important along with the collected data pertaining to the project. Risk mitigation is paramount.
- Require support contractors to obtain risk management training because these people write the information taskers and briefing templates with the common incorrect understandings of the definitions of “risk” and “mitigation” and they are also incorrectly analyzing this information for the decision makers.

2003 - 2012 Sponsored Research Topics

Acquisition Management

- Acquiring Combat Capability via Public-Private Partnerships (PPPs)
- BCA: Contractor vs. Organic Growth
- Defense Industry Consolidation
- EU-US Defense Industrial Relationships
- Knowledge Value Added (KVA) + Real Options (RO) Applied to Shipyard Planning Processes
- Managing the Services Supply Chain
- MOSA Contracting Implications
- Portfolio Optimization via KVA + RO
- Private Military Sector
- Software Requirements for OA
- Spiral Development
- Strategy for Defense Acquisition Research
- The Software, Hardware Asset Reuse Enterprise (SHARE) repository

Contract Management

- Commodity Sourcing Strategies
- Contracting Government Procurement Functions
- Contractors in 21st-century Combat Zone
- Joint Contingency Contracting
- Model for Optimizing Contingency Contracting, Planning and Execution
- Navy Contract Writing Guide
- Past Performance in Source Selection
- Strategic Contingency Contracting
- Transforming DoD Contract Closeout
- USAF Energy Savings Performance Contracts
- USAF IT Commodity Council
- USMC Contingency Contracting

Financial Management

- Acquisitions via Leasing: MPS case
- Budget Scoring
- Budgeting for Capabilities-based Planning
- Capital Budgeting for the DoD
- Energy Saving Contracts/DoD Mobile Assets
- Financing DoD Budget via PPPs
- Lessons from Private Sector Capital Budgeting for DoD Acquisition Budgeting Reform
- PPPs and Government Financing
- ROI of Information Warfare Systems
- Special Termination Liability in MDAPs
- Strategic Sourcing
- Transaction Cost Economics (TCE) to Improve Cost Estimates

Human Resources

- Indefinite Reenlistment
- Individual Augmentation
- Learning Management Systems
- Moral Conduct Waivers and First-term Attrition
- Retention
- The Navy's Selective Reenlistment Bonus (SRB) Management System
- Tuition Assistance

Logistics Management

- Analysis of LAV Depot Maintenance
- Army LOG MOD
- ASDS Product Support Analysis
- Cold-chain Logistics
- Contractors Supporting Military Operations
- Diffusion/Variability on Vendor Performance Evaluation
- Evolutionary Acquisition
- Lean Six Sigma to Reduce Costs and Improve Readiness

- Naval Aviation Maintenance and Process Improvement (2)
- Optimizing CIWS Lifecycle Support (LCS)
- Outsourcing the Pearl Harbor MK-48 Intermediate Maintenance Activity
- Pallet Management System
- PBL (4)
- Privatization-NOSL/NAWCI
- RFID (6)
- Risk Analysis for Performance-based Logistics
- R-TOC AEGIS Microwave Power Tubes
- Sense-and-Respond Logistics Network
- Strategic Sourcing

Program Management

- Building Collaborative Capacity
- Business Process Reengineering (BPR) for LCS Mission Module Acquisition
- Collaborative IT Tools Leveraging Competence
- Contractor vs. Organic Support
- Knowledge, Responsibilities and Decision Rights in MDAPs
- KVA Applied to AEGIS and SSDS
- Managing the Service Supply Chain
- Measuring Uncertainty in Earned Value
- Organizational Modeling and Simulation
- Public-Private Partnership
- Terminating Your Own Program
- Utilizing Collaborative and Three-dimensional Imaging Technology

A complete listing and electronic copies of published research are available on our website: www.acquisitionresearch.net

THIS PAGE INTENTIONALLY LEFT BLANK

ACQUISITION RESEARCH PROGRAM
GRADUATE SCHOOL OF BUSINESS & PUBLIC POLICY
NAVAL POSTGRADUATE SCHOOL
555 DYER ROAD, INGERSOLL HALL
MONTEREY, CALIFORNIA 93943

www.acquisitionresearch.net